DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Delivering Digitally Signed Documents via the Internet

CENDI -- June 13,2001

Keren Cummins, Digital Signature Trust

Agenda

- Background
  - Credentials
  - Benefits of Digital Signatures
  - Mechanics of signing
- Digital Signature Solutions
  - Signing in the Enterprise
  - Individual/Business Signing
  - Signing by an Agency

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Who is DST?

- First licensed CA in the country
- First GSA ACES contract award
- Heavily audited and accredited
- Providing support to NIH, SSA, EPA, FEMA, VA and others
  - GPEA Compliance
  - Risk Assessments
  - Pilots
  - Production Systems
  - Digital Signing Software Assessments and Implementation
- Warranty identity

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Benefits of Digital Signatures

- Authentication
- Message Integrity
- Non-repudiation
- Confidentiality

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Hypothesis:

- STI agencies would like to be able to digitally sign documents that you disseminate to your customers
- Customers would like to be able to:
  - Verify your signature (identify you as the signer and ensure that the document has not been altered in transmission)
  - Validate the certificate (ensure that no one has compromised your identity as the signer)

What's needed to create a digitally signed file?

- The file to be signed
- A private key
  - Associated with your public key in your digital certificate, digitally signed by a CA
- Digital signing software

All of these need to reside on the same computer at the time of signing

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

What's needed to validate a signed file?

- The signed file
- A copy of the digital certificate associated with the private key used to sign the file (contains the public key)

...and...

- Software that verifies the signature
- The ability to validate the certificate (CRL, OCSP, CAM)

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

A Little More on Signing

- Signing email is easy!!! It's built into the major email clients

  … But it's not the same as creating a persistent signed object (archivable)

- Signing documents (.doc, .pdf, XML, HTML) is trickier

  … Requires additional client software to sign, and to handle verification functions

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Needed Signing Solutions

Size of System

Internet Communications (one-to-one)

E-commerce (many-to-one, ad hoc use, multiple work environments)

Enterprise Solutions (intensive peer-to-peer use)

NS Messenger MS Outlook

Emerging Solutions

Most signing solutions available today

$

No client (free, multi-platform, minimal features, can't automate, no workflow)

Minimal client, streamlined features (cheap, multiplatform, allows post-processing)

Full-featured fat client (expensive, proprietary)

DST

DIGITALSIGNATURETRUST

Guaranteeing Identity in Digital Transactions

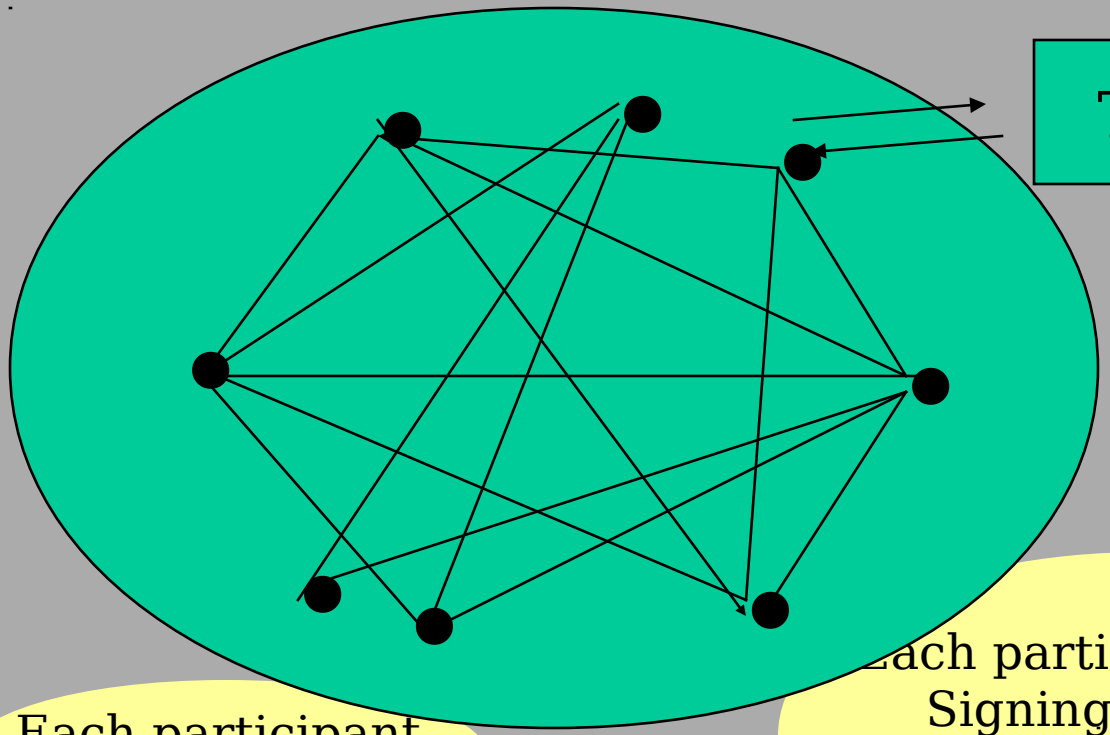
Agenda

- Background
  - Credentials
  - Benefits of Digital Signatures
  - Mechanics of signing
- Digital Signature Solutions
  - Signing in the Enterprise
  - Signing in the GPEA Environment
  - Signing by an Agency for the Public

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Enterprise Environment



Each participant needs a certificate

Each participant needs:
Signing capability
Ability to verify signature
Ability to validate certificat

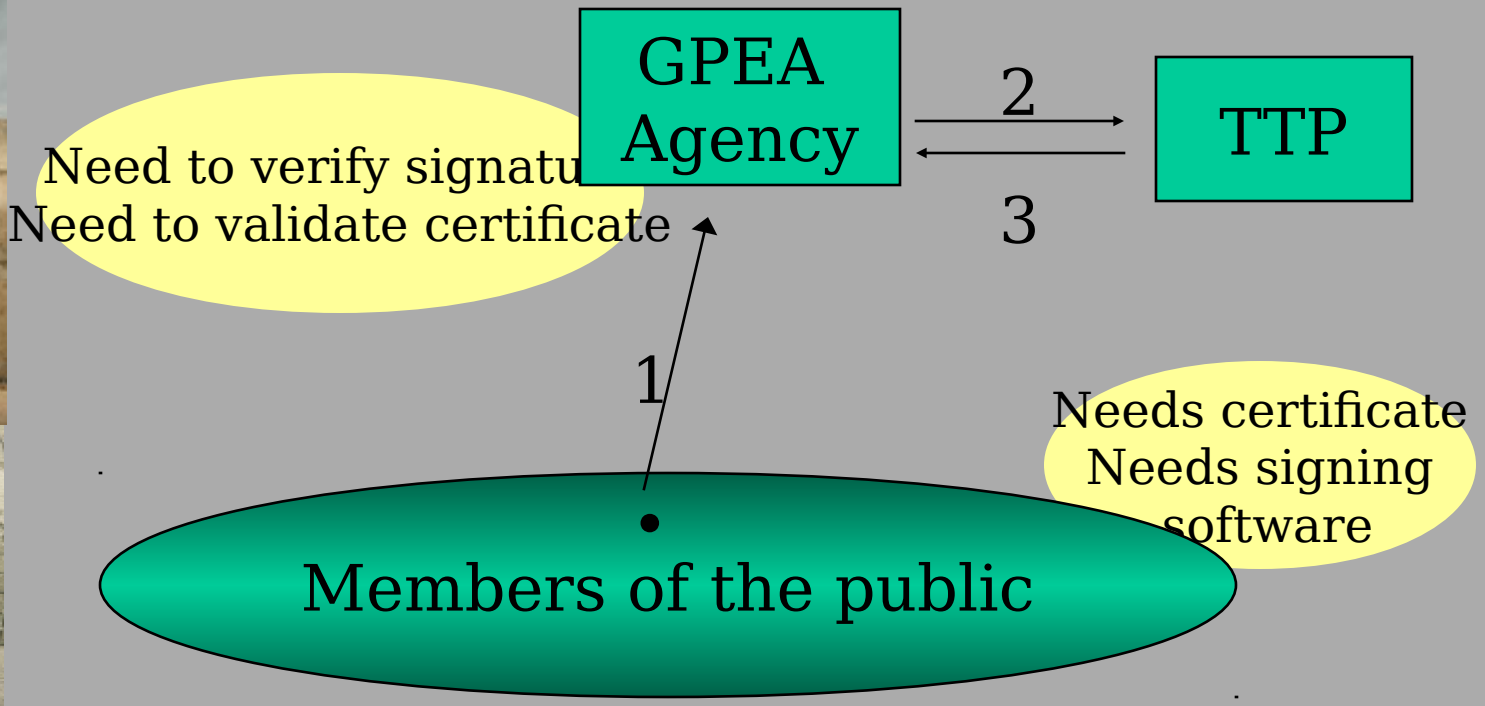
DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Enterprise Signing Req's

- "Many-to-many" interactions
- Users work for common organization
  - Focus on signature verification
  - Cert validation relatively easy
- Large clients are not a problem
  - Organization controls desktop
  - Fully supported software
- Software tends to be feature rich and complicated
  - Most of the signing solutions available today

Typical Agency GPEA Implementation



1. Citizen signs document and uploads to agency
2. Agency verifies signature locally and validates certifica
3. TTP confirms valid certificate

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Individual/Business Interactions with Gov't

- In most cases, constituents sign documents and send them to agency
- Users are unknown, so agencies must validate millions of certs
- Must distribute signing software to millions of users, so software needs to:
  - Have a very small footprint
  - Be easy to use
- ACES contract designed to support this type of implementation

Signing within S&T Community

- Agency may sign few documents which are then downloaded by millions of users
- Validation of signing certificate is important
  - Akin to software signing
  - Threat of downloading malicious code
- Public needs easy and cheap (free) way to validate certificate used to sign the document

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

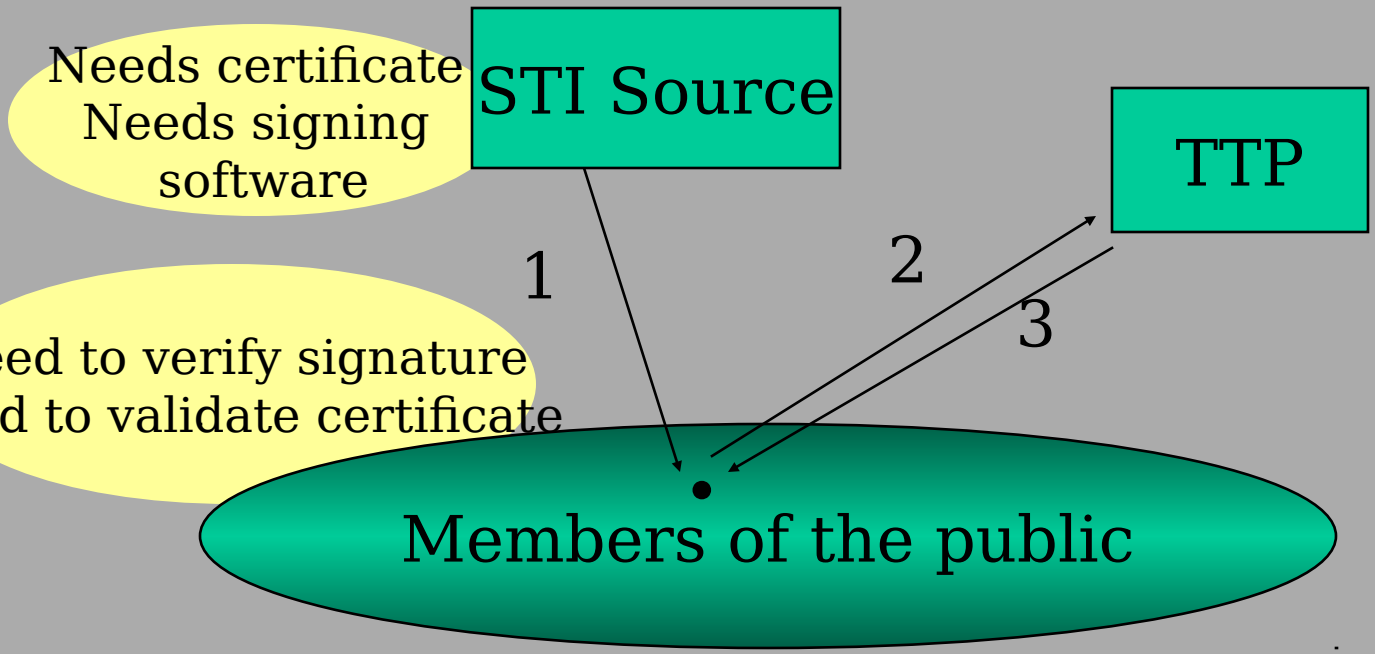
Possible Solution to S&T Signing Problem

- Agency signs documents using enterprise-type software
- Agency certificates are stored in small directory
- Free “readers” are distributed to users
- Readers allow users to verify signature and/or validate cert by checking directory

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Possible STI Solution



1 Customer downloads file from STI source
2 Customer verifies signature locally and then requests certificate
validation from TTP
3 TTP responds with cert validity

DST
DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

STI solution approach

- Follows enterprise model
- Agency signs
- Customer receives signed document
  - Verifies signature
  - Validates certificate

Significant requirements for customer-
Need client on desktop, access to directory, customer expertise

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Advantages of this Approach

- Easy to implement
- and use
- Low cost
- Successfully tested
  - E-SIGN Act digitally signed using DST ACES certificate with E-Lock Assured Office
  - Digitally signed Act and reader can be downloaded at: http://www.elock.com/esign/esignact.htm

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Challenges of this Approach

- Requires customers to install software to check signatures and validate certificates
- Requires agencies to support a directory that can handle a lot of traffic
- Depends on having a well-known and trusted TTP
- Not suited to standard ACES because the public must validate the certificates

DST

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

Conclusions

- Needs of STI community somewhat different than most of e-government
  - Be sure you understand *your* need for PKI
  - Be sure your integrators understand your needs and your *customers capabilities*
  - Select *supporting software* carefully to minimize impact on the public
- Tremendous synergy available to agencies with overlapping constituencies (e.g. research labs)
  - Can share certificate issuance
  - Can share directory support
- Get your certificates from a trusted source!

Questions?

Contact Information:

Keren Cummins

VP, Government Services

Digital Signature Trust Co.

(301) 921-5977

kcummins@trustdst.com

DST

DIGITALSIGNATURETRUST

Guaranteeing Identity in Digital Transactions